ARMY CONTRACT WRITING SYSTEM (ACWS)

Attachment 0014 ACWS_DD_254

Version 1.0

04 April 2016

Solicitation Number: W52P1J-16-R-0058

Prepared By:
Product Manager
Army Contract Writing System (ACWS)

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: Secret

b. LEVEL OF SAFEGUARDING REQUIRED: None

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER: TBD	DUE DATE *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)*: 20150625
	b. REVISED *(Supersedes all previous specs)*	REVISION NO.	DATE *(YYYYMMDD)*
	c. FINAL *(Complete Item 5 in all cases)*		DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD		

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD		

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
TBD		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

The Army Contract Writing System (ACWS) will be the Army's single, next-generation, enterprise-wide contract writing, management, execution, and close-out software system. ACWS will facilitate the standardization of Army Procurement business processes and streamline the integration with Army Enterprise Resource Planning (ERP) systems. ACWS will meet the compliance requirements of the Federal Financial Management Improvement Act (FFMIA) of 1996. The system will meet the full scope of Army Contracting requirements, including those in secure and non-secure locations, those supporting combat or non-combat contingencies, in both CONUS and OCONUS locations.

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X
b. RESTRICTED DATA		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X
d. FORMERLY RESTRICTED DATA		X
e. INTELLIGENCE INFORMATION		
(1) Sensitive Compartmented Information (SCI)		X
(2) Non-SCI		X
f. SPECIAL ACCESS INFORMATION		X
g. NATO INFORMATION		X
h. FOREIGN GOVERNMENT INFORMATION		X
i. LIMITED DISSEMINATION INFORMATION		X
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER *(Specify)*		X

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X	
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. PERFORM SERVICES ONLY		X
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
h. REQUIRE A COMSEC ACCOUNT		X
i. HAVE TEMPEST REQUIREMENTS		X
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
l. OTHER *(Specify)*		X

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release [X] Direct [ ] Through *(Specify)*

Product Manager Army Contract Writing System (PdM ACWS), Suite 9S15, 200 Stovall Street, Alexandria, VA 22322

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

The National Industrial Security Program Operating Manual (NISPOM dated February 2006) applies to this contract. In addition, guidance may be found in DoDI 8500.2 Information Assurance (IA) Implementation, AR-25-2 Information Assurance and DoDI 5200.02, Personnel Security Program for privileged access into systems. Any classified information generated in the performance of this contract shall be classified according to the markings shown on the source material.

10j. Individuals requiring access to privileged DoD Information Technology (IT) systems, sensitive but unclassified data, and/or information marked as "For Official Use Only" will require background investigations commensurate with the level of risk assigned to their duties.

11a. Individuals requiring access to classified information will need a Secret Level Clearance, Interim Secret Clearance will be accepted.

ACWS Security Classification Guide is attached.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [ ] Yes [X] No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. [ ] Yes [X] No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
Oliver Hollingsworth	Security Manager	(703) 806-3715

d. ADDRESS *(Include Zip Code)*	17. REQUIRED DISTRIBUTION	
Program Executive Office Enterprise Information Systems 9350 Hall Road, Bldg 1445 Fort Belvoir, VA 22060	[X]	a. CONTRACTOR
	[X]	b. SUBCONTRACTOR
	[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE	[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	[X]	e. ADMINISTRATIVE CONTRACTING OFFICER
	[X]	f. OTHERS AS NECESSARY PEO EIS Industrial Security Manager

1 CYBERSECURITY

1.1 Nondisclosure of Sensitive and/or Proprietary Data

The Contractor recognizes that in the performance of this TO, it may receive or have access to certain sensitive information, including information provided on a proprietary basis by public or private entities. The Contractor agrees to use and examine this information exclusively in the performance of this TO and to take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government or Government designated support Contractors possessing appropriate proprietary agreements.

1.2 Personnel Security Standards – Refer to policy AR 25-2, AR 380-67, and DoD 5200.2-R for background investigation and clearance

All contractor personnel granted access to classified information released or generated under this task order must be United States citizens with a minimum interim secret security clearance. In addition, access to classified material will be limited to those personnel having not only an appropriate security clearance, but also a valid need to know. The contractor shall appropriately safeguard FOUO information from public disclosure and shall use the FOUO material only for contract performance. Refer to the DD Form 254 for additional information.

Standards designate positions requiring access to IT and for processing information within IT systems. These security designations are required to distinguish potential adverse effects on Army functions and operations and, therefore, the relative sensitivity of functions performed by individuals having certain privileges. These positions are referred to as IT and IT-related positions. The requirements of this section will be applied to all IT and IT-related positions, whether occupied by Department of Army civilian employees, military personnel, consultants, contractor personnel, or others affiliated with the DoD. Additional guidance is available in DOD 5200.2-R.

Personnel requiring access to Information Systems (ISs) to fulfill their duties must possess the required favorable security investigation, security clearance, or formal access approvals, and fulfill any need-to-know requirements. The Contractor shall submit a roster, by name, position, e-mail address, phone number and responsibility, of all staff (including subcontractor staff) working under the task order who require access to ISs. The roster shall be submitted to the COR, with a copy to the Contracting Officer, within 14 calendar days after the effective date of the contract. The Contractor shall notify the Contracting Officer and COR in advance when any new personnel, who are subject to a background check/investigation, will work under the task order and if they have previously been the subject of national agency checks or background investigations. All contractor and subcontractor employees shall comply with the conditions established for their designated position sensitivity level prior to performing any work under this task order.

Investigations are expensive and may delay performance, regardless of the outcome of the investigation. Delays associated with rejections and consequent re-investigations may not be excusable in accordance with FAR clause, Excusable Delays – see FAR 52.249-14. Accordingly, the Contractor shall ensure that any additional employees whose names it submits for work under this task order have a reasonable chance for approval.

The Contractor shall:

- Ensure individuals meet the background investigation and adjudication requirements called for in AR 25-2, AR 380-67, and DoD 2500.2-R.
- Ensure individuals assigned to these sensitive positions have completed the appropriate access request forms.
- Forward employee investigation information to the designated Government Representative before assignment of these individuals on the modification/change order and ensure a visit request with that investigation information is provided yearly.
- Ensure personnel have the proper security clearances, have read and signed the User Agreement, and have completed information technology security training prior to being granted access to networks and/or systems.

IT-I		
Defined as	**IA Positions**	**Security Requirement**
Personnel in an IA positions with privileged-level access to control, manage, or configure IA tools or devices, individual and networked IS and devices, and enclaves.	• System Administrators (SAs)/Network Administrators (NAs) for infrastructure devices IDSs, VPNs, routers • SA/NAs for classified systems and devices	Favorable completion of a National Agency Check (NAC) (current within 180 days). Initiation of a Single Scope Background Investigation (SSBI) and favorable review of SF 85P (Questionnaire For Public Trust Positions), SF 86 (Questionnaire For National Security Positions), and Supplemental Questionnaire.

IT-II		
Defined as	**IA Positions**	**Security Requirement**
Personnel in an IA positions with limited privileged-level access to control, manage, or configure ISs and devices, with very limited (single device) or no IA device access or management.	• Operating system administration of common network applications, or enclaves, back-up operators	A favorable review of local personnel, base/military, medical, and other security records as appropriate. Initiation of a National Agency Check with Local Agency and Credit Checks (NACLC), as appropriate or favorable review of SF85P and Supplemental Questionnaire.

IT-III		
Defined as	**IA Positions**	**Security Requirement**
• Personnel in an IA positions. This is a position of higher trust. • Personnel with roles, responsibilities, and access authorization of normal users with non-privileged level access to the IS or device. • Personnel with non-privileged level access authorization in the role of official or statutory volunteers. The provisions for statutory volunteers are covered in AR 608-1.	• General Users • SA on individual systems for configuration • Management with limited privileged-level access to that IS(s) or device(s)	A favorable review of local personnel, base/military, medical, and other security records as appropriate. Initiation of a National Agency Check (NAC), as appropriate and favorable review of SF85P and Supplemental Questionnaire.

The required investigation levels for an IT-I position are outlined below.

Privileged access – IT-I[1]

User roles	Foreign national	U.S. civilian	U.S. military	U.S. contractor	Conditions or examples
DAA or IAPM	Not allowed	SBBI	SBBI	Not allowed	None
IANM	Not allowed	SBBI	SBBI	Conditional SSBI	With CIO/G-6 written approval, contractors may continue as IA personnel until replaced
IAM	Not allowed	SBBI	SBBI	Conditional SSBI	Contractor may not fill MSC, installation, or post IAM position
IASO/IANO	Not allowed	SBBI	SBBI	Conditional SSBI	None
Monitoring or testing	Not allowed	SBBI	SBBI	SSBI	Examples: administration of IA devices (for example, boundary devices, IDSs, routers, and switches)
SA/NA or Administrator (with IV privileged access) or maintenance of IA devices	Conditionally allowed – SSBI (equivalent)[2]	SBBI	SBBI	SSBI	

Notes:

[1]Investigative levels are defined in DOD 5200.2-R. The term "Foreign National" (FN) refers to all individuals who are non-U.S. citizens, including U.S. military personnel, DOD civilian employees, and contractors.
[2]FN-under the immediate supervision of a U.S. citizen with written approval of CIO/G-6.

Limited privileged access – IT-II[1]

User roles	FN (see note 2)	U.S. civilian	U.S. military	U.S. contractor	Conditions or examples
IAM/IANM	Not allowed	NACI	NACLC	NACLC	None
IANO/IASO	Conditionally allowed-NACLC equivalent	NACI	NACLC	NACLC	FN-with DAA written approval, and documentation in the C&A package, direct or indirect hires may continue as IA personnel until they are replaced, provided they serve under the immediate supervision of a U.S. citizen IAM and have no supervisory duties
Supervisor of IT I or IT II positions	Not allowed	NACI	NACLC	NACLC	None
Administrator (with no IA privileged access) or maintenance of IA-enabled products	Conditionally allowed-NACLC equivalent[2]	NACI	NACLC	NACLC	Examples: IS administration, OS administration, end-user administration, and administration of common applications (for example, e-mail, word processing)

Notes:
[1]Investigative levels are defined in DOD 5200.2-R. FN refers to all individuals who are non-U.S. citizens, including U.S. military personnel, DOD civilian employees, and contractors.
[2]FN-under the immediate supervision of a U.S. citizen.

1.3 Non-US Citizen in IT Positions

Performance by non-U.S. citizens in IT positions shall be minimized. However, compelling reasons may exist to grant access to DoD IT resources in those circumstances in which a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable U.S. citizen is not available. Access to sensitive information by a non-U.S. citizen who is not a DoD employee will only be permitted IAW applicable disclosure policies (e.g., National Disclosure Policy 1, DoD Directive (DoDD) 5230.9, DoDD 5230.25) and US statutes (e.g., the Arms Export Control Act, 22 USC 39). Non-U.S. citizens assigned to DoD IT positions are subject to the investigative requirements outlined below. For positions identified as IT - II and III, foreign nationals may be appointed if they: 1) possess a unique or unusual skill or expertise that is urgently needed for a specific DoD requirement and for which a suitable United States citizen is not available, and 2) are approved in writing by the PEO EIS as the Agency Director. However, under no circumstances can these individuals be assigned before

completion and favorable adjudication of the appropriate security investigation. In all cases the Contractor shall forward employee investigation information to the COR before employees are assigned to work under a specific TO. The Contractor will ensure that a Visit Request is forwarded to the COR for each location where employees will be assigned. That Visit Request must be provided on an annual basis.

1.4 Right to Require Removal

The Government retains the right to require removal of Contractor personnel, regardless of prior clearance or adjudication status, whose actions while assigned to this TO conflict with the interests of the Government. The reason for removal will be fully documented in writing by the Contracting Officer.

1.5 Privacy Act

Data processed at PEO EIS locations may contain Privacy Act information which requires the reading, signing, and adherence to appropriate nondisclosure documents. Contractor personnel shall sign and return a Non-Disclosure Agreement to the COR prior to commencing work.

1.6 Identification

Contractor personnel attending meetings, answering Government telephones, and working in other situations where their contract status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by Contractors are suitably marked as Contractor products or that Contractor participation is appropriately disclosed. Contractor personnel will be required to wear and clearly display an identification badge with their full name and corporate affiliation at all times while performing Government-site duties.

2 ANTITERRORISM (AT) AND OPERATIONS SECURITY (OPSEC)

Use of the term ‘Contractor’ shall include subcontractor(s), and the use of the term ‘Contractor employee(s)’ shall include subcontractor employee(s).

2.1 AT Level I Training

Contractor employees requiring access to Government installations, facilities, or controlled access areas shall complete AT level I awareness training within 30 calendar days after TO start date or addition of new Contractor employees. The Contractor shall submit certificates of completion for each affected Contractor employee to the Contracting Officer’s Representative within 5 calendar days after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at https://atlevel1.dtic.mil/at.

2.2 Access and General Protection / Security Policy and Procedures

Contractor employees shall comply with applicable installation, facility, and area commander installation and facility access and local security policies and procedures (provided by the government representative). The Contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services, or Security Office. Contractor employees must comply with all personal identity verification requirements as directed by DoD, HQDA, and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in Contractor security matters or processes.

2.3 iWATCH Training

Contractor shall brief all employees on the local iWATCH program (training standards provided by the requiring activity AT Officer). This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to immediately report suspicious activity to installation security of local law enforcement personnel. The COR will be notified of each suspicious activities reporting incident within 30 calendar days of each incident. This training shall be completed within 30 calendar days of TO award and within 30 calendar days of new employees commencing performance. The Contractor shall submit evidence of completion for each affected Contractor employee to the COR within 30 calendar days after completion of training.

2.4 Contractor Employees Who Require Access to Government Information Systems

Contractor employees with access to a Government information system shall be registered in ATCTS at commencement of services and must successfully complete the DoD Information Assurance Awareness training prior to access to the information system and then annually thereafter.

2.5 Contractors that Require OPSEC Training

Per AR 530-1, Operations Security, new Contractor employees shall complete Level I OPSEC training within 30 calendar days of reporting for duty. All Contractor employees must complete annual OPSEC awareness training.

2.6 IA / IT Training

Contractor employees shall complete the DoD IA awareness training before issuance of network access and annually thereafter. All Contractor employees working IA/IT

functions shall comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M, and AR 25-2.

2.7 IA / IT Training Certification

Per DoD 8570.01-M, DFARS 252.239.7001, and AR 25-2, all contractor employees supporting IA/IT functions shall be appropriately certified upon TO award. The baseline certification as stipulated in DoD 8570.01-M shall be completed upon TO award.

2.8 Handling or Access to Classified Information

Contractor shall comply with FAR 52.204-2, Security Requirements and all other applicable requirements specified in the TO. This clause applies when access to information classified as Confidential or Secret is required by the TO.